ZILKA·KOTAB
PC
ZILKA, KOTAB & FEECE™

95 SOUTH MARKET ST., SUITE 420
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	July 7, 2005	**Phone Number**	**Fax Number**
To:	Patent Appeals, USPTO		(703) 872-9306
From:	Kevin J. Zilka		

Docket No.: NAI1P065/01.307.01 **App. No: 10/029,686**

Total Number of Pages Being Transmitted, Including Cover Sheet: 34

Message:

Please deliver to the Board of Patent Appeals.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Erica
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

July 6, 2005

Practitioner's Docket No. NAI1P065/01.307.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: H.Joiner

Application No.: 10/029,686 Group No.: 2135
Filed: 12/21/2001 Examiner: Son, Linh L. D.
For: COMPREHENSIVE ENTERPRISE NETWORK ANALYZER, SCANNER AND INTRUSION DETECTION FRAMEWORK

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION–37 C.F.R. § 41.37)

1. Transmitted herewith is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on May 13, 2005.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*
(When using Express Mail, the Express Mail label number is mandatory; Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ **(mandatory)**

TRANSMISSION

✓ facsimile transmitted to the Patent and Trademark Office, (703) _____ - _____

Date: 7/7/2005

Erica L. Farlow
Signature

Erica L. Farlow
(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R.1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$500.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $500.00 to Deposit Account No. 50-1351 (Order No. NAI1P065).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P065).

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of	)
	)
H. Joiner	) Group Art Unit: 2135
	)
Application No. 10/029,686	) Examiner: Son, Linh L.D.
	)
Filed: 12/21/2001	) Docket No. NAI1P065_01.307.01
	)
For: COMPREHENSIVE ENTERPRISE NETWORK ANALYZER, SCANNER AND INTRUSION DETECTION FRAMEWORK	) Date: July 7, 2005

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on May 13, 2005.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS

IV STATUS OF AMENDMENTS

V SUMMARY OF CLAIMED SUBJECT MATTER

VI ISSUES

VII ARGUMENTS

VIII APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

Since no such proceedings exist, no Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-37

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-37
3. Claims allowed: None
4. Claims rejected: 1-37

C. CLAIMS ON APPEAL

The claims on appeal are: 1-37

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1 et al., a system for analyzing a network, scanning the network, and detecting intrusions in the network is provided including a plurality of agents coupled to a plurality of computers interconnected via a network. Each agent is adapted to collect information (e.g. items 402 and 900 of Figure 14 et al.). Additionally included is a plurality of host controllers coupled to the agents for collecting the information from the agents, scanning the information, and detecting intrusions in the network (e.g. item 1002 of Figure 14 et al.). Still yet, a plurality of zone controllers coupled to the host controllers are included for analyzing an output of the host controllers, and executing security actions in response thereto (e.g. item 1602 of Figure 16). A report is also generated including a plurality of objects in a tree representation (e.g. item 2401 of Figure 24). Further, intrusion detection services are provided based on the information and a Simple Network Management Protocol (SNMP) trap capability is utilized. Note page 28, lines 8-26 and page 29, line 24-page 33, line 11, for example.

With respect to a summary of Claim 22 et al., a method is provided for business rule-based network services utilizing a network, which includes collecting information relating to a plurality of computers utilizing a plurality of agents coupled to the computers via a network. Also included is collecting the information from the agents utilizing a plurality of controllers coupled to the agents. Further a plurality of business rules are identified and services are provided utilizing the information based on the business rules. Additionally, a report is generated including a plurality of objects in a tree representation (e.g. item 2401 of Figure 24), intrusion detection services are provided based on the information, and a Simple Network Management Protocol (SNMP) trap capability is utilized. Note page 28, lines 8-26 and page 29, line 24-page 33, line 11, for example.

VI ISSUES (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1, 3-6, 8-11, 13-16, 18-22 and 25-37 under 35 U.S.C. 103(a) as being unpatentable over Drake et al., U.S. Patent No. 6,347,374, in view of Porras et al., U.S. Patent No. 6,704,875.

Issue # 2: The Examiner has rejectcd Claims 2, 7, 12, 17, 23 and 24 under 35 U.S.C. 103(a) as being unpatentable over Drake in view of Porras, and further in view of Eschelbeck (U.S. Patent No. 6,553,378).

VII ARGUMENTS (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue #1:

The Examiner has rejected Claims 1, 3-6, 8-11, 13-16, 18-22 and 25-37 under 35 U.S.C. 103(a) as being unpatentable over Drake et al., U.S. Patent No. 6,347,374, in view of Porras et al., U.S. Patent No. 6,704,875.

Group #1: Claims 1, 3, 6, 8, 11, 13, 16, 18, 21 and 25-28

Specifically, with respect to Claim 1, the Examiner has admitted that Drake does not teach "a plurality of zone controllers coupled to the host controllers for analyzing an output of the host controllers, and executing security actions in response thereto." Despite the prior art's failure to disclose the above claim language, the Examiner has rejected such language by stating that "[i]t is obvious at the time of the invention for one of ordinary skill in the art to separate both components to minimize the processing time and load."

Applicant respectfully asserts that it would not have simply been obvious for one of ordinary skill in the art to separate both the host controllers and the zone controllers, as claimed by applicant. Specifically, Drake does not disclose any separate controller for "analyzing an output of the host controllers," and "executing security actions in response thereto." Applicant argues that separate zone controllers capable of analyzing and executing security actions, as claimed by applicant, provide for specific advantages not met by the prior art.

Not only do the separate zone controllers minimize processing time and load as the Examiner has suggested, but separate zone controllers also provide a complete solution of monitoring and detecting problems on a corporate enterprise level without requiring modules on every switch in the network since the zone controllers are each associated with a plurality of host controllers. In addition, this provides a solution that may fully scale to any size corporate network. Furthermore, the zone controllers are adapted to be associated with certain zones within a network. Applicant notes that the foregoing advantages are only some of the advantages of maintaining separate host and zone controllers, and that for these and other reasons such separation would not have been obvious to one of ordinary skill in the art.

In the latest response of April 25, 2005, the Examiner argues "it is obvious for one having ordinary skill in the art to make the modification to separate or delegate functionalities to multiple processors environment" and that the "processing delegation is a popular method to minimize the processor load and processing time." Applicant respectfully disagrees.

Specifically, nowhere in the prior art is there any disclosure, teaching or even suggestion of separating controllers in the specific manner claimed by applicant, namely "a plurality of zone controllers coupled to the host controllers for analyzing an output of the host controllers, and executing security actions in response thereto." In addition, the prior art completely fails to provide for the advantages of applicant's specific claim language listed hereinabove. Therefore, appellant respectfully asserts that it would not have been obvious to separate or delegate functionality, as the Examiner contends, especially in view of the specific manner in which applicant claims utilization of multiple controllers.

Furthermore, in the response of April 24, 2005, the Examiner also argues that, in Drake, the ESG has many functionalities and one of which is the auditing parsing (Col. 7, line 26). The Examiner continues to state that the auditing parsing has similar functionalities as the HC, such as collecting the information from the agents, scanning the information, and detecting intrusions (Col. 7, lines 24-54). Furthermore, the Examiner states that the output of the raw event records gets converted to Virtual Records and that the Expert system engine has functionalities similar to the ZC (Col. 11, lines 7-67) such that the ZC scans through the database, which is the output of the HC, and then executes the response thereto (Col. 11, lines 25-65).

In making such a statement, the Examiner has failed to address applicant's claimed "plurality of host controllers...for collecting the information from the agents, scanning the information, and detecting intrusions in the network" (emphasis added). Simply nowhere in the prior art is there any disclosure of a host controller that scans information. It seems the Examiner has relied on Drake's teaching of a parser to meet applicant's claimed host controllers, but simply nowhere in Drake is there even any mention of a parser that scans information.

Further, the Examiner states that the expert system engine functions as appellant's claimed zone controller. However, in making such a statement, the Examiner has failed to consider the full weight of applicant's claim language. Specifically, applicant claims that the host controller detects intrusions in the network and the zone controller executes security actions in response thereto. Drake, on the other hand, discloses that the expert system engine analyzes the virtual records and detects attack signatures (see Col. 11, lines 58-66). In summary, Drake's expert system engine simply detects the intrusions, as does appellant's host controller, but does not execute security actions in response thereto, as does appellant's zone controller. Thus, Drake's expert system engine clearly cannot meet appellant's zone controller and the associated specific claimed functionality.

Still yet, the Examiner has admitted that Drake does not teach applicant's claimed technique "wherein a report is generated including a plurality of objects in a tree representation." The Examiner has stated that a "report in a tree representation is the designer choice." Applicant respectfully asserts that a report in a tree representation is not simply a designer choice since not all information is capable of being displayed in that way. For instance, Drake specifically teaches reports utilizing bar charts and reports in tabular format (see Col. 17, lines 25-59), but fails to disclose any report "including a plurality of objects in a tree representation," as claimed by applicant. Thus, Drake's invention does not support the creation of reports in a tree representation and therefore such would simply not be a designer choice.

In the response of April 25, 2005, the Examiner again states that it is a designer's choice to formulate the report that is best to apprehend. Applicant again respectfully asserts that not all information is capable of being displayed in a tree representation, and thus is not simply a designer choice. Different report formats are designed to report different types of information. For instance, bar charts are designed to compare things, whereas line charts show the linear representation of information, and tree representations have various benefits. In this way, Drake's disclosure of bar charts could not possibly be converted into a tree representation since the format of information being reported is entirely different and therefore could not be reported simply based on a designer's choice.

Even still yet, the Examiner has relied on Porras (col. 3 line 15 to Col. 4, line 67; Col. 7 line 18-Col. 8, line 67) to meet applicant's claimed "wherein a Simple Network Management Protocol (SNMP) trap capability is utilized." Applicant respectfully asserts that the only mentioning of SNMP in Porras is in relation to "networks being monitored...include[ing] features common to many network operating systems such as...SNMP..." (col. 3, lines 46-54) and "the monitors 22 may format their respective

alert streams in a variety of formats, such as...SNMP..." (col. 4, lines 1-3). The Examiner has not only mistakenly relied on such excerpts since they relate to types of networks being monitored and to formats of alerts, but has also mistakenly relied on (Col. 7, line 18-Col. 8 line 67) which altogether fails to even mention SNMP, let alone an SNMP trap capability. Thus, "wherein a Simple Network Management Protocol (SNMP) trap capability is utilized," as claimed by applicant, is simply not met by the prior art.

In the response of April 25, 2005, the Examiner argues that Porras does specify that the security and fault-monitoring system comprises SNMP (col. 3, lines 45-60). Applicant asserts that, in fact, Porras merely teaches that the "[n]etwork services occurring within the networks 12-16 include features common to many network operating systems such as...SNMP" (see specifically col. 3, lines 50-54). Thus, there is clearly no teaching of utilizing an SNMP trap capability, in the manner claimed by applicant, since Porras simply teaches that SNMP is included in the network services.

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. In re Vaeck,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met since the combination of Drake and Porras fail to teach all of applicant's claim limitations, as noted above.

Group #2: Claims 4 5, 9, 10, 14, 15, 19 and 20

The Examiner has relied on col. 17, lines 15-24 of Drake to meet applicant's claimed technique "wherein the host controllers and the zone controllers operate based on business rules." Applicant respectfully asserts that the above excerpt from Drake merely teaches a configuration update and the maintenance of static database tables, neither of which deal with the operations of the host controllers and zone controllers, as claimed.

Again, applicant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met since the combination of Drake and Porras fail to teach all of applicant's claim limitations, as noted above.

Group #3: Claim 22

The Examiner has relied on the same rejection as that given with respect to independent Claims 1, 6, 11, 16 and 21, along with Drake's disclosed "specifics of implementation...var[y] based on an audit source" (Col. 5, lines 36-60) and Drake's disclosed functionality of a "manager/configuration GUI" (Col. 17, lines 1-24). In relying on such excerpts from Drake, the Examiner has failed to address the claim language of Claim 22 not incorporated into the other above mentioned independent Claims, namely:

"identifying a plurality of business rules;" and
"providing services utilizing the information based on the business rules."

Applicant respectfully asserts that Drake's teachings of audit analysis and of a manager/configuration GUI, as mentioned above, simply do not even suggest "business

rules" in the manner claimed by applicant. Specifically, there is simply no mention in Drake of utilizing business rules in any way, and especially not to "provid[e] services utilizing the information based on business rules."

In response of April 25, 2005, the Examiner states that col. 17, lines 5-24 of Drake include the business rule, such as user account logs, etc. Appellant respectfully asserts that the above excerpt from Drake simply teaches configuration and maintenance of static databases. Such teaching does not meet applicant's claimed "providing services utilizing the information based on the business rules," since the only business rules that could be found in Drake relate to configuring static tables and not to providing services in the manner claimed by applicant.

Again, applicant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met since the combination of Drake and Porras fail to teach all of applicant's claim limitations, as noted above.

Group #4: Claim 29

The Examiner has relied on col. 8, line 43-col. 9, line 15 of Drake to make a prior art showing of applicant's claimed technique "wherein enterprise latency mapping is performed." Applicant respectfully asserts that the above excerpt from Drake only teaches that "audit data can be acquired and processed using either of the following modes: (a) batch mode; (b) real time mode." Thus, Drake only teaches latency with respect to a batch mode in that audit data is only periodically passed by a collector to a downstream process, but not that any sort of latency mapping is performed, as claimed by applicant.

Again, applicant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met since the combination of Drake and Porras fail to teach all of applicant's claim limitations, as noted above.

Group #5: Claim 30

The Examiner has relied on col. 2, lines 12-17 of Porras to make a prior art showing of applicant's claimed technique "wherein at least one of the zone controllers chooses a port number associated with an application." Applicant respectfully asserts that the above excerpt from Porras merely teaches an alert manager that can listen to a specific port. Such alert manager only relates to managing alerts and thus does not meet applicant's zone controller.

In addition, applicant respectfully points out that simply listening to a specified port, as disclosed in Porras, does not meet applicant's claimed technique "wherein at least one of the zone controllers chooses a port number associated with an application" because Porras fails to even mention choosing the specific port according to an application associated with the port, wherein a zone controller performs the choosing.

Again, applicant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met since the combination of Drake and Porras fail to teach all of applicant's claim limitations, as noted above.

Group #6: Claims 31 and 32

The Examiner has relied on col. 11, line 7-col. 12, line10 and col. 16, line 53-57 of Drake to meet applicant's claimed technique "wherein the at least one zone controller pushes a configuration request to a plurality of the host controllers in an associated zone." The Examiner also states that the "agent (Collector) sends the event info based

on the expert system requests." Applicant respectfully asserts that simply sending event info, as the Examiner relies on, does not rise to the level of specificity of applicant's claimed configuration request.

In addition, Drake's mere mention of a configuration GUI simply does not rise to the level of specificity of applicant's claim language, since applicant clearly claims a zone controller pushing "a configuration request to a plurality of the host controllers in an associated zone" and a "host controller push[ing] the configuration request to the agents" (emphasis added).

Again, applicant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met since the combination of Drake and Porras fail to teach all of applicant's claim limitations, as noted above.

Group #7: Claim 34

The Examiner has relied on col. 10, lines 10-20 and col. 11, lines 5-25 of Drake to make a prior art showing of applicant's claimed "wherein monitor data is sent from the agents to the host controllers." Applicant respectfully asserts that the excerpts from Drake merely teach raw audit data, Virtual Records, data about existing events, and new events. Simply nowhere in Drake is there any mention of monitor data such that the monitor data is sent from agents to host controllers.

Again, applicant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met since the combination of Drake and Porras fail to teach all of applicant's claim limitations, as noted above.

Group #8: Claim 35

The Examiner has relied on Drake's disclosure of a "generalized database storage architecture" (Col. 5, lines 20-30) to make a prior art showing of applicant's claimed "wherein the monitor data is buffered." Simply stating that database storage is utilized does not inherently require data to be buffered, and furthermore, the entire Drake reference fails to make any suggestion of buffering monitored data.

Again, applicant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met since the combination of Drake and Porras fail to teach all of applicant's claim limitations, as noted above.

Group #9: Claim 36

The Examiner has relied on Drake's disclosure of "a set of graphical user interfaces" (Col. 16, lines 53-67; Fig. 1, item 16) to make a prior art showing of applicant's claimed "wherein the host controllers update the at least one zone controller with consolidated monitor data." Drake specifically teaches a GUI that "allows update of selected fields" (see Fig. 1, item 16), but such fields relate to configuration of the event detection system. Applicant respectfully asserts that such disclosure in no way relates to "host controllers updat[ing] the at least one zone controller with consolidated monitor data".

Again, applicant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met since the combination of Drake and Porras fail to teach all of applicant's claim limitations, as noted above.

Group #10: Claim 37

The Examiner has relied on col. 8, line 43-col. 9, line 15 of Drake to make a prior art showing of applicant's claimed technique "wherein differences in delay times are calculated to construct a picture of latency throughout an enterprise." Applicant

respectfully asserts that the above excerpt from Drake merely teaches that "audit data can be acquired and processed using either of the following modes: (a) batch mode; (b) real time mode." Thus, Drake only teaches latency with respect to a batch mode in that audit data is only periodically passed by a collector to a downstream process, but not that any sort of delay times are calculated to construct a picture of latency through an enterprise, as claimed by applicant.

Again, applicant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met since the combination of Drake and Porras fail to teach all of applicant's claim limitations, as noted above.

Issue #2:

The Examiner has rejected Claims 2, 7, 12, 17, 23 and 24 under 35 U.S.C. 103(a) as being unpatentable over Drake in view of Porras, and further in view of Eschelbeck (U.S. Patent No. 6,553,378).

Group #1: Claims 2, 7, 12, 17, 23 and 24

These claims are deemed allowable for the reasons base Claim 1 is deemed allowable.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII APPENDIX OF CLAIMS (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A system for analyzing a network, scanning the network, and detecting intrusions in the network, comprising:
(a) a plurality of agents coupled to a plurality of computers interconnected via a network, each agent adapted to collect information;
(b) a plurality of host controllers coupled to the agents for collecting the information from the agents, scanning the information, and detecting intrusions in the network; and
(c) a plurality of zone controllers coupled to the host controllers for analyzing an output of the host controllers, and executing security actions in response thereto;
wherein a report is generated including a plurality of objects in a tree representation;
wherein intrusion detection services are provided based on the information;
wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.

2. (Original) The system as recited in claim 1, wherein the host controllers are further capable of cybercop services.

3. (Original) The system as recited in claim 1, wherein the zone controllers are further capable of integrated reporting.

4. (Original) The system as recited in claim 1, wherein the host controllers and the zone controllers operate based on business rules.

5. (Original) The system as recited in claim 1, wherein the business rules are user-configurable.

6. (Previously Presented) A method for analyzing a network, scanning the network, and detecting intrusions in the network, comprising:

(a) collecting information relating to a plurality of computers utilizing a plurality of agents coupled to the computers via a network;

(b) collecting the information from the agents utilizing a plurality of host controllers coupled to the agents;

(c) scanning the information utilizing the host controllers;

(d) detecting intrusions in the network utilizing the host controllers;

(e) collecting the information from the host controllers utilizing a plurality of zone controllers coupled to the host controllers;

(f) analyzing output of (b)-(d) utilizing the zone controllers; and

(g) executing security actions based on the analysis utilizing the zone controllers;

wherein a report is generated including a plurality of objects in a tree representation;

wherein intrusion detection services are provided based on the information;

wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.

7. (Original) The method as recited in claim 6, wherein the host controllers are further capable of cybercop services.

8. (Original) The method as recited in claim 6, wherein the zone controllers are further capable of integrated reporting.

9. (Original) The method as recited in claim 6, wherein the host controllers and the zone controllers operate based on business rules.

10. (Original) The method as recited in claim 6, wherein the business rules are user-configurable.

11. (Previously Presented) A computer program product for analyzing a network, scanning the network and detecting intrusions in the network, comprising:

(a) computer code for collecting information relating to a plurality of computers utilizing a plurality of agents coupled to the computers via a network;

(b) computer code for collecting the information from the agents utilizing a plurality of host controllers coupled to the agents;

(c) computer code for scanning the information utilizing the host controllers;

(d) computer code for detecting intrusions in the network utilizing the host controllers;

(e) computer code for collecting the information from the host controllers utilizing a plurality of zone controllers coupled to the host controllers;

(f) computer code for analyzing output of (b)-(d) utilizing the zone controllers; and

(g) computer code for executing security actions based on the analysis utilizing the zone controllers;

wherein a report is generated including a plurality of objects in a tree representation;

wherein intrusion detection services are provided based on the information;

wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.

12. (Original) The computer program product as recited in claim 11, wherein the host controllers are further capable of cybercop services.

13. (Original) The computer program product as recited in claim 11, wherein the zone controllers are further capable of integrated reporting.

14. (Original) The computer program product as recited in claim 11, wherein the host controllers and the zone controllers operate based on business rules.

15. (Original) The computer program product as recited in claim 14, wherein the business rules are user-configurable.

16. (Previously Presented) A system for analyzing a network, scanning the network and detecting intrusions in the network, comprising:

(a) agent means adapted to collect information;

(b) host controller means for collecting the information from the agent means, scanning the information, and detecting intrusions in the network; and

(c) zone controller means for analyzing an output of the host controller means, and executing security actions in response thereto;

wherein a report is generated including a plurality of objects in a tree representation;

wherein intrusion detection services are provided based on the information;

wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.

17. (Original) The system as recited in claim 16, wherein the host controller means is further capable of cybercop services.

18. (Original) The system as recited in claim 16, wherein the zone controller means is further capable of integrated reporting.

19. (Original) The system as recited in claim 16, wherein the host controller means and the zone controller means operate based on business rules.

20. (Original) The system as recited in claim 19, wherein the business rules are user-configurable.

21. (Previously Presented) A system for analyzing a network, scanning the network, and detecting intrusions in the network, comprising:

(a) a plurality of agents coupled to a plurality of computers interconnected via a network, each agent adapted to collect information;

(b) a plurality of host controllers coupled to the agents for collecting the information from the agents;

(c) means for scanning the information;

(d) means for detecting intrusions in the network;

(e) a plurality of zone controllers coupled to the host controllers for analyzing an output of the host controllers; and

(f) means for executing security actions in response to at least one of the scanning, the detecting, and the analyzing;

wherein a report is generated including a plurality of objects in a tree representation;

wherein intrusion detection services are provided based on the information;

wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.

22. (Previously Presented) A method for providing business rule-based network services utilizing a network, comprising:

(a) collecting information relating to a plurality of computers utilizing a plurality of agents coupled to the computers via a network;

(b) collecting the information from the agents utilizing a plurality of controllers coupled to the agents;

(c) identifying a plurality of business rules; and

(d) providing services utilizing the information based on the business rules;

wherein a report is generated including a plurality of objects in a tree representation;

wherein intrusion detection services are provided based on the information;

wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.

23. (Original) The method as recited in claim 22, wherein the services include analysis services, intrusion detection services, anti-virus services, and security services.

24. (Original) The method as recited in claim 22, wherein the services include at least one of analysis services, intrusion detection services, anti-virus services, and security services.

25. (Previously Presented) A system for analyzing a network and detecting intrusions in the network, comprising:
a plurality of information collectors coupled to a plurality of computers interconnected via a network, each information collector adapted to collect information;
at least one information collector manager coupled to the information collectors for collecting the information from the information collectors, and detecting intrusions in the network; and
a user interface for analyzing an output of the information collector manager;
wherein a report is generated including a plurality of objects in a tree representation;
wherein intrusion detection services are provided based on the information;
wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.

26. (Original) The system as recited in claim 25, wherein the information relates to wireless network traffic.

27. (Previously Presented) A method for analyzing a network and detecting intrusions in the network, comprising:
collecting information relating to a plurality of computers utilizing a plurality of information collectors coupled to the computers via a network;
collecting the information from the information collectors utilizing at least one information collector manager coupled to the information collectors; and
detecting intrusions in the network based on an analysis utilizing the information;
wherein security actions are capable of being carried out based on the analysis;
wherein a report is generated including a plurality of objects in a tree representation;
wherein intrusion detection services are provided based on the information;
wherein a Simple Network Management Protocol (SNMP) trap capability is utilized.

28. (Original) The method as recited in claim 27, wherein the information relates to wireless network traffic.

29. (Previously Presented) The system as recited in claim 1, wherein enterprise latency mapping is performed.

30. (Previously Presented) The system as recited in claim 29, wherein at least one of the zone controllers chooses a port number associated with an application.

31. (Previously Presented) The system as recited in claim 30, wherein the at least one zone controller pushes a configuration request to a plurality of the host controllers in an associated zone.

32. (Previously Presented) The system as recited in claim 31, wherein the host controllers push the configuration request to the agents.

33. (Previously Presented) The system as recited in claim 32, wherein the agents monitor a port associated with the port number.

34. (Previously Presented) The system as recited in claim 33, wherein monitor data is sent from the agents to the host controllers.

35. (Previously Presented) The system as recited in claim 34, wherein the monitor data is buffered.

36. (Previously Presented) The system as recited in claim 34, wherein the host controllers update the at least one zone controller with consolidated monitor data.

37. (Previously Presented) The system as recited in claim 36, wherein differences in delay times are calculated to construct a picture of latency throughout an enterprise.

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P065_01.307.01).

Respectfully submitted,

By: _____ Date: 7/7/05

Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660